EXHIBIT 2

1
Version: 2.0
Date: 01/06/2020

StoneX Group Inc.
Standard ITC-015

Control

Acceptable Use of IT Facilities

1.0 Purpose

This *Control Standard* supports the **Information Security Policy** and sets the responsibilities and required behaviour of users of the Company's information systems, networks and computers, collectively known as IT resources.

2.0 Scope

All staff (including contractors and interns), members of organisations who have been granted access to use the Company's IT resources are subject to this *Control Standard*, collectively known as 'Users'.

3.0 Control Statements

3.1 General

Users must not carry out any action that shall or may interfere with the normal working of the IT resources or may interfere with or disrupt other users' use of the IT resources or access, corrupt or modify any other user's data without their consent.

Users must not deliberately introduce a virus, worm, trojan horse, Spyware, or other similar code nor take any action to circumvent, or reduce the effectiveness of, any anti-virus or other malicious software detection, removal and protection precautions established by the Company.

Users are responsible for all use of their username. Users should not make their username or password available to anyone else nor should they use any other person's username.

Users must not install games on Company owned computers. The Company will block any games traffic that negatively affects other users' experience and will not provide support for any gaming activities.

Users must not tamper with the configuration of any Company computer or any cables or peripheral devices attached to Company computers.

Users must at all times adhere to the policies and procedures of the Company, in addition to all applicable laws.

3.2 Legal Requirements and Prohibited Use

Users shall not use IT resources in any way which could expose themselves or the Company to any criminal or civil liability. Users who fail to abide by the following rules may be subject to disciplinary action, up to and including termination of employment.

IT Facilities shall be used in accordance with the following:

- **software** - software should always be used in accordance with the terms of the relevant licence and copying software without the licence holder's permission is prohibited.
- **rights in content** - do not use third party text, images, sounds, trademarks and logos in any materials e.g. emails, documents and web pages without the consent of the rights holder. Consent must be verified and approved by the Marketing or Legal team.
- **offensive material** – users must not use the IT resources to access, store or distribute material that is obscene, indecent or pornographic. If the Company suspects a user has accessed material that might give rise to criminal liability, it may notify local law enforcement.
- **discrimination and harassment** - Users must not create, distribute or access material that is unlawfully discriminatory, including on the grounds of age, sex, sexual orientation, race, gender identity, disability, religion/belief, or any other protected characteristic; that is likely to incite any form of violence or hatred; or that is likely to cause harassment, alarm or distress.
- **computer misuse** - unauthorised access to accounts (including stealing or misusing a password), programs and/or data and all forms of hacking are prohibited and may be an offence under local Laws and regulations.
- **defamation** – users should take care to avoid content which may be defamatory. Particular care is needed when sending material electronically or by posting material to the Internet (e.g., through web pages, or social media).
- **data** – all data owned, processed or held by the Company, must be accessed, stored, processed and backed up in a manner appropriate to its security classification. Failure to appropriately classify and handle data is a breach of this Policy.
- **personal data** - data on living persons must be held and processed in accordance with Laws and regulations (e.g. General Data Protection Regulation - GDPR). Persons who hold Personally Identifiable Information must control and process these data in accordance with the data protection principles.
- **formation of contracts** - users should note that it is possible to form contracts electronically, without any hard copy confirmation from the user. Care should be taken to obtain appropriate authority before declaring to commit the Company to any contractual obligations (which may include clicking 'I agree' to an online dialogue box) and the wording 'subject to contract' should be

used on emails where appropriate.

- **unsolicited and offensive e-mail** – users must not send unsolicited e-mail or other mass e-mails (spam) to multiple recipients, except as part of legitimate Company activities, including sanctioned marketing campaigns and research. Users must not send e-mail that any person of the Company may reasonably find offensive or likely to cause annoyance or needless anxiety. This includes a prohibition on forwarding on chain letters, advertisements, or replying inappropriately to an entire mailing list.

3.3 Monitoring and Privacy

The Company shall act in accordance with applicable legislation and regulatory requirements in relation to the monitoring of communications. As such, the Company may log all forms of IT use and communications. Monitoring systems is necessary for administrators to identify and investigate technical and security related problems, and also provides an audit log in the event of user misconduct or criminal investigations.

The Company also reserves the right to inspect any items of computer equipment connected to the network. Any IT equipment connected to the Company's network will be removed if it is deemed to be breaching Company policy or otherwise interfering with the operation of the network.

The Company may need to access or suspend any user's account for business purposes. Action will only be taken where it has been authorised by a suitable HR representative.

3.4 Personal Use

The Company recognises that users may make personal use of Company systems, including email and the Internet. Personal use should be reasonable and not excessive, ensuring that it does not interfere with IT resources, business requirements or any other Company or legislative requirement.

Users are allowed to make personal use of the IT resources and services only if such use:

- does not interfere with the performance of their daily tasks and job function
- does not incur unwarranted expense on the Company
- does not have a negative impact on the Company; and
- is otherwise in accordance with these conditions of use.

It is not recommended that users store or share their own sensitive data for personal use on Company systems as the Company cannot guarantee the confidentiality, integrity or availability of this information.

The Company reserves the right to withdraw access to IT resources for personal use at any time and may remove or modify information (including personal data) held on its IT resources.

3.5 Connecting Devices to Company Networks

In order to reduce risks of malware infection and propagation, risks of network disruption and to ensure compliance with Information Security policies. It is permissible to connect personally owned equipment to the Company's wireless *guest* networks; however, it is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose.

To further reduce risk of data loss, members of staff shall not connect any personally owned peripheral device which is capable of storing data (for example, a personally owned USB stick) to any Company owned equipment, irrespective of where the equipment is located. Only Company owned peripheral devices may be connected to Company owned equipment.

3.6 Use of Services Provided by Third Parties

Users must only use services provided or endorsed by the Company for conducting Company business. The Company recognises, however, that there are occasions when it is unable to meet the legitimate requirements of its Users. In these circumstances Users are required to submit a vendor assessment request to the IT Governance (ITG) team for review and approval.

3.7 Unattended Equipment

Computers and other equipment used to access Company IT resources must not be left unattended and unlocked if logged in. Users must ensure that their computers are locked before being left unattended. Care should be taken to ensure that no sensitive/restricted information is left on display on the computer when it is left unattended.

For further information please refer to the **Clear Desk and Screen** *Control Standard*.

Particular care must be taken to ensure the physical security of Company supplied equipment when in transit.

For further information please refer to the **Mobile and Remote Working** *Control Standard.*

3.8 Exit Procedures

Upon leaving the Company it is expected that users:

- promptly return all Company IT equipment in reasonable working condition
- do not delete any data which belongs to the Company
- transfer any data which may be needed by the Company to an appropriate server or colleague prior to departure
- ensure any of their own data that they wish to keep is removed from the Company's systems, as they will not be entitled to access this once they leave
- review and conform to any other procedures set out by the Company in relation to departure

4.0 Penalties for Misuse

Minor breaches of this *Standard* will be dealt with by IT Services. Heads of Department may be informed of the fact that a breach of policy has taken place. More serious breaches (or repeat offenders) may be dealt with under the Company's disciplinary procedures. Where applicable, breaches of the law may be reported to local Law enforcement agencies.

Document Control

Title	Acceptable Use of IT Facilities
Owner	IT Governance
Author	David Hall – Senior IT Governance Risk & Compliance Analyst
Contributors	Jim Richey - Global Head of Human Resources, Catherine Odigie – Head of Legal, AJ King – Director, IT Security
Protective Marking	Internal
Review Period	Each Calendar Year
Target Audience	All Staff, Regulators, Contractors and Vendors

Version History

Version	Date	Description	Reviewer(s)	Approver
0.1	September 2011	Draft	Lisa Leonard	
1.0	January 2013	Initial release	Lisa Leonard	Lisa Leonard
1.1	October 2018	Review period updated	-	David Hall
2.0	01/06/2020	Updated legal content and to new Service Now version	Jim Richey, Catherine Odigie, AJ King	Abbey Perkins

It is the responsibility of Senior Management to ensure that any policies and procedures relating to this document or their area of responsibility are effectively communicated, implemented and monitored.

This document forms part of StoneX's Information Security Governance Framework and as such cannot be changed in any way without formal approval. To propose a change to this document, a request for change is required to be submitted to the document owner for review and approval.

Distribution of this document outside of the company is controlled and as such all requests are to be submitted to the IT Governance department for approval.

ACKNOWLEDGEMENT AND RECEIPT

I acknowledge that I have received and read the StoneX Group Inc. Acceptable Use Policy.

Employee Signature: Howard Shipman

Printed Name: Howard Shipman

IP Address: [redacted]

Date: 2/8/2021

It is the responsibility of Senior Management to ensure that any policies and procedures relating to this document or their area of responsibility are effectively communicated, implemented and monitored.

This document forms part of StoneX's Information Security Governance Framework and as such cannot be changed in any way without formal approval. To propose a change to this document, a request for change is required to be submitted to the document owner for review and approval.

Distribution of this document outside of the company is controlled and as such all requests are to be submitted to the IT Governance department for approval.